

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X
ENIGMA SOFTWARE GROUP USA, LLC,

Plaintiff,

-against-

MALWAREBYTES INC.,

Defendant.

Case No. 1:16-cv-07885 (PAE)

FIRST AMENDED COMPLAINT

-----X
Plaintiff Enigma Software Group USA, LLC (“ESG”), by its attorneys, for its First Amended Complaint against Defendant Malwarebytes Inc., formerly known as Malwarebytes Corporation (“Malwarebytes”), respectfully alleges as follows:

SUMMARY OF THE CASE

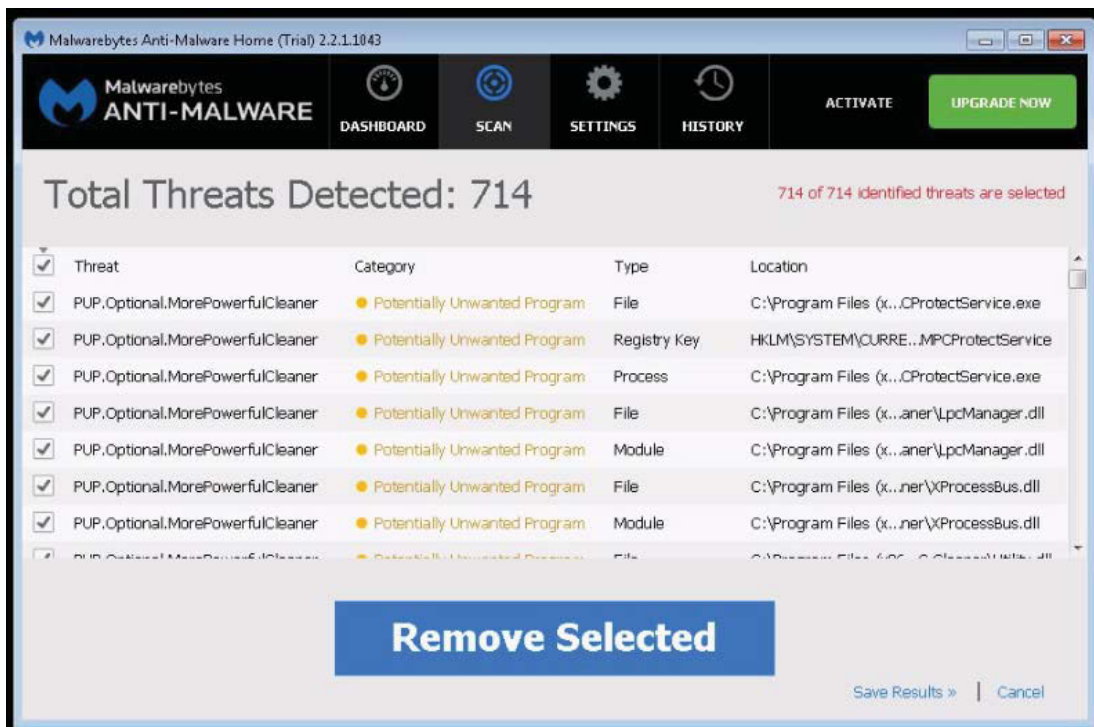
1. This is an action for civil remedies, including injunctive relief and damages, under the federal Lanham Act and the laws of the State of New York, arising out of the unlawful, predatory and bad faith practices of Malwarebytes, a direct competitor of ESG, aimed at unfairly competing with ESG in the market for anti-malware and Internet security software.

2. ESG develops and markets computer security software that detects and removes malicious software (*i.e.*, malware), which includes, *inter alia*, viruses, spyware and adware; enhances Internet privacy; and eliminates other security threats. ESG’s products protect millions of customers from an array of serious risks, including computer hacks, system breaches, identity theft, and system computing malware, as well as other computer and Internet security threats.

3. Malwarebytes, a self-professed industry leader, has since 2008 provided consumers with anti-malware and Internet security software aimed at protecting consumers' computers from malware.

4. Malwarebytes profits from and directly competes with ESG in the anti-malware and Internet security market. Its flagship product known as Malwarebytes Anti-Malware ("MBAM") directly competes with ESG's flagship product known as SpyHunter. Malwarebytes promotes MBAM as a consumer solution that detects and removes malware on personal computers in the United States and worldwide.

5. Historically, Malwarebytes' MBAM has purported to detect "Potentially Unwanted Programs" or "PUPs," which are automatically quarantined and flagged as "threats" for MBAM's users. Below is an example of MBAM's "Threat Scan Results" on a computer infected with malware. As the screenshot illustrates, the user is shown over 700 purported "threats," every one of which is preselected for removal from the user's system:



6. From its inception in 2008 through October 4, 2016—and in the face of eight years of direct competition between Malwarebytes and ESG—Malwarebytes never identified ESG’s SpyHunter program, ESG’s advanced Windows registry cleaner and PC optimizer called RegHunter, or any other ESG product as a PUP or any other type of malware and it never quarantined or blocked installation of any of ESG’s programs.

7. However, on October 5, 2016, Malwarebytes unilaterally revised the “criteria” it uses to identify PUPs and announced the revision to the public through a blog post by its CEO. Ex. 1. This was Malwarebytes’ first announced change in its PUP criteria since 2013, and the new “policy” included only subjective criteria that Malwarebytes could, and has, implemented at its own malicious whim to identify SpyHunter and RegHunter as PUPs and “threats.”

8. Specifically, Malwarebytes’ new purported criteria are purposefully and directly aimed at harming ESG by, *inter alia*, interfering with ESG’s current and prospective customer base, injuring ESG’s business, and retaliating against ESG for its lawsuit against Bleeping Computer LLC (“Bleeping”), as explained below.

9. Upon announcement of the new PUP criteria, Malwarebytes’ MBAM product began identifying SpyHunter and RegHunter as PUPs, meaning that Malwarebytes began falsely flagging ESG’s programs as “threats” to the consuming public even though these highly regarded ESG programs are legitimate and pose no security threat to users’ computers.

10. For example, if a consumer already has SpyHunter or RegHunter on his or her computer and then downloads and scans his or her computer with MBAM, MBAM automatically identifies SpyHunter and RegHunter as PUPs and automatically quarantines the programs. Once MBAM quarantines SpyHunter and RegHunter, MBAM prevents the user—even if he or she tries to “restore” SpyHunter or RegHunter—from launching or using SpyHunter and RegHunter

on his or her computer without undertaking several additional steps that may not be readily apparent to, or understood by, a novice user.

11. In addition, if a consumer already has MBAM installed on his or her computer and tries to download and install SpyHunter or RegHunter, MBAM blocks the installation of the ESG programs, regardless of whether the user attempts to “restore” SpyHunter and RegHunter from quarantine.

12. On October 19, 2016, Malwarebytes acquired AdwCleaner, an anti-adware product that purports to identify and remove PUPs, adware, toolbars, and other unwanted software for its users. *See* Ex. 2.

13. At the time of its acquisition by Malwarebytes, AdwCleaner did not identify SpyHunter or RegHunter as PUPs or any other type of malware and did not remove those programs.

14. However, on or about October 27, 2016—just one week after its acquisition by Malwarebytes—AdwCleaner, like MBAM, began identifying, detecting, quarantining, and blocking SpyHunter and RegHunter as PUPs in furtherance of Malwarebytes’ purposeful anti-competitive conduct to directly injure ESG’s business and as part of Malwarebytes’ retaliation for ESG’s lawsuit against Bleeping, as described below. *See* Ex. 3.

15. By identifying SpyHunter and RegHunter as PUPs, Malwarebytes is falsely representing to the consuming public that ESG’s programs are a “threat” and that their computers’ security will be compromised if they download and install SpyHunter or RegHunter or do not remove the programs from their computers.

16. Moreover, as described herein, Malwarebytes, through its MBAM and AdwCleaner products, unilaterally blocks consumers from installing and using ESG’s products.

In addition, Malwarebytes deactivates ESG's products on consumers' computers *who already have previously installed and paid for* those products.

17. By unjustifiably and unlawfully identifying SpyHunter and RegHunter as PUPs, preselecting them for removal, and—even if a user attempts to restore SpyHunter and RegHunter—defaulting back to identifying them as PUPs and automatically selecting them for removal every time the user scans his or her computer with MBAM or AdwCleaner, Malwarebytes is unilaterally disrupting and/or disabling ESG's existing and prospective customers' attempts to use SpyHunter or RegHunter—for which the customers pay subscription fees to ESG—to protect their computers from cyberattacks, viruses, hackers, and other threats.

18. The fact that ESG's customers deliberately download and confirm that they want to pay for SpyHunter and RegHunter belies Malwarebytes' supposed detection of these programs as “potentially unwanted.”

19. Malwarebytes' unlawful conduct in preventing ESG from providing its existing and prospective customers truly free choices as to the cybersecurity protections that they want for their computers is all the more egregious in the current climate of highly-publicized computer hacking, financial fraud and identity theft occurring around the world on a daily basis.

20. Malwarebytes knows that detecting and quarantining as PUPs the products of a competitor, like ESG, causes immediate harm to the competitor in the form of lost sales and revenues and also causes irreparable harm to the competitor's business reputation as a result of being identified as a “threat” that a consumer should either not install or should remove from his or her computer. Malwarebytes also knows that a decision to identify SpyHunter and RegHunter as PUPs is likely to result in other anti-malware companies following suit, which swiftly causes exponentially more harm to ESG.

21. Malwarebytes' deliberate decision to change its PUP criteria and begin falsely identifying SpyHunter and RegHunter as PUPs was not coincidental. Rather, in addition to being part of Malwarebytes' anti-competitive, predatory scheme to deliberately injure ESG and harm its existing and prospective customers, it was a bad faith decision Malwarebytes made to retaliate against ESG for pressing forward with a factually-related lawsuit against Bleeping that is currently pending before this Court (*Enigma Software Group USA, LLC v. Bleeping Computer LLC et al.*, Case No. 1:16-cv-00057 (PAE) (S.D.N.Y. Mar. 18, 2016)) (the "Bleeping Lawsuit"), and, more specifically, for seeking to discover the true business/commercial relationship between Bleeping and Malwarebytes through service upon Malwarebytes of a subpoena to produce documents in that case (the "Subpoena").

22. Malwarebytes and Bleeping have an affiliate relationship by which Bleeping promotes the MBAM product and earns commissions from Malwarebytes if a consumer purchases MBAM through a link on Bleeping's website.

23. In the Bleeping Lawsuit, ESG alleges that Bleeping has engaged in a deliberate scheme of disseminating false, misleading and inaccurate information about ESG and its SpyHunter product and instructing consumers not to install, or to uninstall, SpyHunter and instead purchase Malwarebytes' competing MBAM product, thereby promoting Malwarebytes' business interests and earning revenues for itself and for Malwarebytes while damaging ESG.

24. The Subpoena ESG served on Malwarebytes sought documents revealing the extent of Malwarebytes' involvement in Bleeping's unlawful smear campaign against ESG.

25. Just one week before it was required by law to respond to the Subpoena, Malwarebytes revised its PUP definition to consider subjective criteria including purported

“predominantly negative feedback or ratings from the user community” that it could implement at its own malicious whim to identify SpyHunter and RegHunter as PUPs. *See* Ex. 4.

26. Bleeping has attempted to defend its unlawful conduct in the Bleeping Lawsuit by asserting that it acted in reliance on some supposed negative feedback on ESG’s products from some unidentified “user community,” which includes Bleeping and its “staff,” Malwarebytes, and some of Malwarebytes’ high-level employees and/or executives.

27. Malwarebytes’ transparent attempt to bolster Bleeping’s defense in the Bleeping Lawsuit—to Malwarebytes’ ultimate benefit—and to further harm ESG shows the extent to which Bleeping and Malwarebytes act in concert to promote their mutual interests.

28. The charade that is Malwarebytes’ “changed” PUP criteria was quickly recognized as such by members of the Bleeping and Malwarebytes “communities,” who all-but publicly acknowledged Malwarebytes’ bad faith conduct and its connection to the Bleeping Lawsuit.

29. For example, on October 5, 2016, Malwarebytes’ CEO Marcin Kleczynski announced on the Forums webpage of Malwarebytes’ website that Malwarebytes had “made some changes to [its] PUP detection criteria.” Ex. 4. The first question came from a Bleeping “Special Ops Tech” and “Trusted Advisor” posting under the name *Aura*, who asked “what was added/removed/edited.” *Id.* In response, Malwarebytes explained that “[t]he biggest change” in the PUP criteria was that it now considers “predominantly negative feedback or ratings from the user community.” *Id.* *Aura* replied: “Guessed as much[.]” *Id.*

30. Within hours of Malwarebytes’ public announcement, Bleeping owner Lawrence Abrams posted a news story on the front page of Bleeping’s website lauding Malwarebytes’ new policy and copying verbatim Malwarebytes’ “updated PUP criteria.” Exs. 5 & 6.

31. Bleeping “Security Colleague” *Angoid* commented on Abrams’ front-page news story with a thinly-veiled admission that Malwarebytes’ policy was directed specifically at ESG and SpyHunter, given Bleeping’s history of attacking ESG and the ongoing Bleeping Lawsuit. Specifically, *Angoid* stated: “What would be really strange is if anyone can think of any other anti-malware program that fits any one of those descriptions [the PUP criteria] not that I can think of one of course :).” Ex. 6.

32. Moreover, on or about October 27, 2016, AdwCleaner developer Jérôme Boursier, who joined the Malwarebytes team as a special engineer and researcher upon AdwCleaner’s acquisition, posted the following to his Twitter account:



Ex. 3.

33. The following day, Malwarebytes forum “New Member” *rhabdomantist* posted a link to Boursier’s October 27, 2016 Twitter post to the Forums webpage of Malwarebytes’ website under the thread Home > Malwarebytes Tools and Other Products > Malwarebytes AdwCleaner > SpyHunter RemovalFrom Twitter. Ex. 7. Malwarebytes “Expert” *David H. Lipman* responded: “Nice way to exacerbate things when Enigma has already filed suit against Malwarebytes. It’s one thing quietly removing Enigma’ware. It is another announcing it, in public, after a suit has already been filed.” *Id.* *rhabdomantist* replied that the Twitter post had been made by AdwCleaner’s developer (*i.e.*, Boursier), to which *David H. Lipman* responded:

Right. **WHY** tweet it?

If there are 15,1000 [sic] PUPs that are current, should we expect 15,000 tweets for each and every one? It isn’t like some major BOTnet takedown or something of that nature.

Why exacerbate the issue after a lawsuit was filed in US Federal Court?

Id. (original emphasis).

34. ESG brings this lawsuit and, if necessary, will move for preliminary injunctive relief to put an immediate stop to the damage and irreparable harm that Malwarebytes has intentionally and maliciously caused and continues to cause to both ESG and the consuming public as a result of its bad faith campaign of unfair competition and false and misleading statements identifying SpyHunter and RegHunter as PUPs and “threats” and thereby deceiving consumers and interfering with ESG’s customer relationships.

THE PARTIES

35. Plaintiff ESG is a Florida limited liability company, having merged with a Connecticut limited liability company of the same name. ESG does business in this district.

36. Upon information and belief, Defendant Malwarebytes is a corporation organized under the laws of Delaware and headquartered at 3979 Freedom Circle, 12th Floor, Santa Clara, CA 95054. Malwarebytes was originally incorporated under the laws of Delaware on January 6, 2014 as Malwarebytes Corporation. On December 21, 2015, Malwarebytes filed a Restated Certificate of Incorporation with the Delaware Secretary of State that amended the company name to Malwarebytes, Inc.

37. Malwarebytes currently employs a Regional Vice President in the greater New York City area. *See* Ex. 8. At least five Malwarebytes employees work remotely from their homes in New York.

38. As of October 6, 2016, Malwarebytes was seeking to hire a Senior Sales Engineer in New York to work with the Regional Sales Manager to “present[] Malwarebytes[] security solution to prospective customers” and “work closely with customers as their primary point of feedback and resolution of issues.” Ex. 9.

39. Upon information and belief, Malwarebytes advertises, provides its software for download and installation, and has sold its software to consumers residing in New York, including in this District.

40. Malwarebytes is misleading and deceiving consumers in New York and this District by wrongly detecting SpyHunter and RegHunter as PUPs. At least twenty (20) ESG customers who, upon information and belief, reside in New York have reported to ESG Technical Support that Malwarebytes’ MBAM and/or AdwCleaner products have detected, quarantined and blocked their SpyHunter and/or RegHunter programs as PUPs and some have requested refunds from ESG. Upon information and belief, at least three (3) of those customers reside in this District, two in New York County and one in Bronx County.

JURISDICTION AND VENUE

41. This action arises under the Lanham Act, 15 U.S.C. § 1051 *et seq.*, and the laws of the State of New York. This Court has subject matter jurisdiction pursuant to, *inter alia*, 28 U.S.C. §§ 1331, 1332, 1338, and 1367.

42. Upon information and belief, this Court has personal jurisdiction over Malwarebytes because Malwarebytes (i) regularly transacts business in New York and this District; (ii) has committed tortious acts in New York and this District by wrongly detecting, quarantining and blocking SpyHunter and RegHunter as PUPs when Malwarebytes' software runs scans on computers physically located in this State and District; (iii) has committed tortious acts that have misled and deceived consumers in New York and this District and have disrupted and disabled their use of ESG's programs, which tortious acts Malwarebytes should reasonably expect would have consequences in this State; and (iv) derives substantial revenue from international commerce.

43. Malwarebytes has intentionally availed itself of the privilege of conducting business in New York and this District; purposefully directed activity at this State and District by providing its software for download and purchase to New York consumers and detecting, quarantining and blocking New York consumers' SpyHunter and RegHunter programs; and created sufficient minimum contacts with this State and District such that Malwarebytes can reasonably and fairly anticipate being haled into this Court.

44. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)–(c) because Malwarebytes is subject to personal jurisdiction in, and so resides in, this District.

FACTS

ESG and Malwarebytes Compete in the Anti-Malware and Internet Security Market

45. ESG is led by Alvin Estevez, who previously worked for a military defense contractor of the United States Government, where he gained vast experience in complex data systems and computer security and learned the importance of cybersecurity and the immense risks of cyberattacks. Estevez has been featured multiple times as a cybersecurity expert in Forbes Magazine and other national publications.

46. ESG has spent more than a decade combatting malware. Its flagship anti-malware software program is known as SpyHunter, which is presently in version 4. SpyHunter is an adaptive malware detection and removal tool that provides rigorous protection against the latest malware threats, including spyware, Trojans, rootkits, and other malicious software.

47. RegHunter is ESG's advanced Windows registry cleaner and PC optimizer software program. It repairs, restores and boosts the performance of computers running the Windows operating system by removing registry errors, cleaning computer file clutter, defragmenting hard drives, and other optimizations.

48. Consumers can download a free scanning version of SpyHunter through a link entitled "Download Free Scanner." The scanner detects whether a computer has malware or other threats.

49. Consumers also have the choice to buy a license to the full version of SpyHunter, and ESG provides consumers with a "Buy Now" link. The full version of SpyHunter includes the scanner, tools to remove malware, and other security protection tools.

50. ESG sells licenses to SpyHunter and RegHunter solely over the Internet, including at its website, <<http://www.enigmasoftware.com>>.

51. ESG enjoys worldwide sales of SpyHunter and RegHunter, including sales to residents of New York.

52. ESG's SpyHunter and RegHunter products have received top industry certifications and have both been certified as TRUSTe Certified Downloads.

53. ESG is a Better Business Bureau accredited business. Better Business Bureau accreditation standards include a "commitment to make a good faith effort to resolve any consumer complaints." ESG has received an "A+" rating from the Better Business Bureau.

54. Malwarebytes is a direct competitor of ESG in the anti-malware and Internet security market. MBAM is consumer software that detects and removes malware on personal computers in the United States and worldwide.

55. MBAM operates by scanning a user's computer for malware and other computer security threats, detecting any such threats, reporting to the user the results of the detection, and then taking remedial action, such as preventing a malicious download, removing the threat from the computer, or providing the user with an option to remove the detected program.

56. Malwarebytes acquired AdwCleaner, an anti-adware software program, on October 19, 2016. *See, e.g.,* Ex. 2. Malwarebytes announced the acquisition on its website that day, touting AdwCleaner as "one of the world's most frequently downloaded tools for removing potentially unwanted programs (PUPs), adware, toolbars and other unwanted software." *Id.* Malwarebytes boasts that AdwCleaner is downloaded by "[c]onsumers and businesses ... more than 200,000 times per day, making it one of the most downloaded products on many sites," having been downloaded "around 200 million times[.]" *Id.*

57. In its October 19, 2016 acquisition announcement, Malwarebytes also noted that AdwCleaner developer Boursier and co-developer Corentin Chepeau would be "join[ing]

Malwarebytes in engineering and research roles.” *Id.* Malwarebytes CEO Kleczynski similarly blogged on Malwarebytes’ website about its AdwCleaner acquisition, Boursier and Chepeau.

Ex. 10. Boursier blogged on his personal website, <<https://fr33tux.org>>: “I’m now part of Malwarebytes.” Ex. 11.

58. Malwarebytes offers free downloads of its MBAM and AdwCleaner products on its website at < <https://www.malwarebytes.com/mwb-download/>> and <<https://www.malwarebytes.com/adwcleaner/>>, respectively. It also sells its “Premium” MBAM product on its homepage, <<https://www.malwarebytes.com/>>.

59. Malwarebytes advertises its free MBAM product as having nine distinct technical capabilities (*e.g.*, “Anti-Malware/Anti-Spyware,” “Advanced malware removal,” and “Malicious website blocking”). Five of the nine capabilities expire after 14 days of free use. To retain use of those five capabilities, a consumer must purchase the Premium MBAM product.

60. Upon information and belief, Malwarebytes’ intention in offering its free MBAM and AdwCleaner downloads is to preview its products’ capabilities and entice consumers to ultimately purchase the Premium MBAM product. In this way, the free MBAM and AdwCleaner downloads are marketing tools for Malwarebytes.

ESG Files Suit Against Bleeping and Serves a Subpoena on Malwarebytes

61. On January 5, 2016, ESG filed the Bleeping Lawsuit seeking redress for Bleeping’s pattern and practice of making false and misleading statements about ESG to drive consumers away from purchasing ESG’s products, including SpyHunter, and toward purchasing Malwarebytes’ products, including MBAM. The details of Bleeping’s smear campaign against ESG are laid out in full in ESG’s Second Amended Complaint (ECF No. 25).

62. As alleged in the Bleeping Lawsuit, Malwarebytes directly profited and continues to profit from Bleeping's false and misleading statements about ESG, which drive customers away from ESG's products and to Malwarebytes' products.

63. Malwarebytes will be a witness in the Bleeping Lawsuit.

64. Malwarebytes and/or its CEO have financially supported Bleeping in the Bleeping Lawsuit by directly providing money to Bleeping in response to Bleeping's GoFundMe campaign to raise money for its defense costs.

65. ESG and Bleeping began fact discovery in the Bleeping Lawsuit after the Court denied Bleeping's motion to dismiss ESG's Second Amended Complaint, finding, *inter alia*, that the alleged false and misleading statements "unmistakably constitute advertisements" for Malwarebytes (ECF No. 45).

66. On September 7, 2016, as part of fact discovery, ESG served Malwarebytes with the Subpoena pursuant to Rule 45 of the Federal Rules of Civil Procedure. The Subpoena sought the production of documents, information, or objects reflecting the nature of Malwarebytes' relationship with Bleeping and the extent of its involvement in Bleeping's smear campaign against ESG.

67. In accordance with the Subpoena's request for compliance within 35 days of service, Malwarebytes was required by law to produce documents responsive to the Subpoena by October 12, 2016. To the extent it had objections to the Subpoena, Malwarebytes had fourteen days to provide those written objections to ESG under Rule 45(d)(2) of the Federal Rules of Civil Procedure.

68. On October 11, 2016—three weeks *after* the deadline for objections had passed and only one day before its substantive response to the Subpoena was due—Malwarebytes

served objections on ESG. Malwarebytes had not contacted ESG to request additional time to object or even to indicate that Malwarebytes was planning to object. Ultimately, Malwarebytes produced a single document in response to the Subpoena, admitting that it did not even search for other responsive documents.

69. As a result, ESG was forced to file a motion to compel Malwarebytes' production of documents responsive to the Subpoena. ESG filed the motion, including a request that the motion be transferred to this Court, on November 16, 2016, in the United States District Court for the Northern District of California (*i.e.*, the court where compliance is required) (*Enigma Software Group USA, LLC v. Bleeping Computer LLC, et al.*, Case No. CV-16-80243 (MISC) (N.D. Cal. Nov. 16, 2016)).

70. To date, Malwarebytes has provided no further response to the Subpoena. Rather, it has chosen to pursue its new line of attack on ESG.

Malwarebytes Revises its PUP Criteria to Bolster Bleeping's Defense and Harm ESG

71. Before October 5, 2016, Malwarebytes had never designated SpyHunter, RegHunter, or any other ESG program as a PUP or any other type of "threat" for which its programs scan, despite the fact that MBAM and SpyHunter have coexisted and competed in the market for over seven years. This means that, to the extent any of the PUP criteria announced by Malwarebytes on October 5, 2016 were used by Malwarebytes prior to that date, SpyHunter and RegHunter did not meet those criteria.

72. Less than a week before Malwarebytes should have responded to the Subpoena, thereby revealing the extent of its involvement in Bleeping's unlawful conduct, Malwarebytes began directly interfering with ESG's relationships with existing and prospective customers, making false statements about ESG's SpyHunter and RegHunter products under the guise of having revised its PUP criteria.

73. On October 5, 2016, MBAM announced that it had changed its PUP criteria, which it identified in total as: (1) “obtrusive, misleading, or deceptive advertising, branding, or search practices”; (2) “excessive or deceptive distribution, affiliate or opt-out bundling practices”; (3) “aggressive or deceptive behavior especially surrounding purchasing or licensing”; (4) “unwarranted, unnecessary, excessive, illegitimate, or deceptive modifications of system settings or configuration (including browser settings and toolbars)”; (5) “difficulty uninstalling or removing the software”; (6) “predominantly negative feedback or ratings from the user community”; (7) “diminishes user experience”; and (8) “other practices generally accepted as riskware, scareware, adware, greyware, or otherwise commonly unwanted software by the user community.” Ex. 12; *see also* Exs. 1 & 4.

74. Malwarebytes further “reserve[d] the right to adjust, expand and update [its] criteria” for PUP identification “without prior notice or announcements.” Ex. 12.

75. Unsurprisingly, Malwarebytes’ announced PUP criteria track the various defenses Bleeping is asserting against ESG in the Bleeping Lawsuit.

76. Upon information and belief, Malwarebytes specifically designed its vague and unbounded criteria as a pretense to begin blocking its users’ access to SpyHunter and RegHunter at its malicious whim in order to bolster Bleeping’s defenses in the Bleeping Lawsuit and/or to influence ESG to stop pursuing the Bleeping Lawsuit—to the clear advantage of Malwarebytes, given its affiliate relationship with Bleeping and the outstanding Subpoena—and to damage ESG’s business for anticompetitive purposes.

77. Demonstrating the connection between Malwarebytes’ conveniently-timed revision to its PUP criteria and the Bleeping Lawsuit, Bleeping placed Malwarebytes’ changed criteria on the front page of its website, <www.bleepingcomputer.com>, on the very same day

that Malwarebytes made its announcement. *See* Exs. 5 & 6. Bleeping titled that main story: “Malwarebytes going to battle with PUPs and Adware.” *Id.*

78. Moreover, AdwCleaner developer and now Malwarebytes engineer and researcher Boursier made clear in his October 27, 2016 Twitter post the true intent of Malwarebytes’ revised PUP criteria. Boursier broadcast with enthusiasm: “#AdwCleaner by @Malwarebytes now fully detects and removes #SpyHunter from Enigma Software Group. #PUP.” Ex. 3.

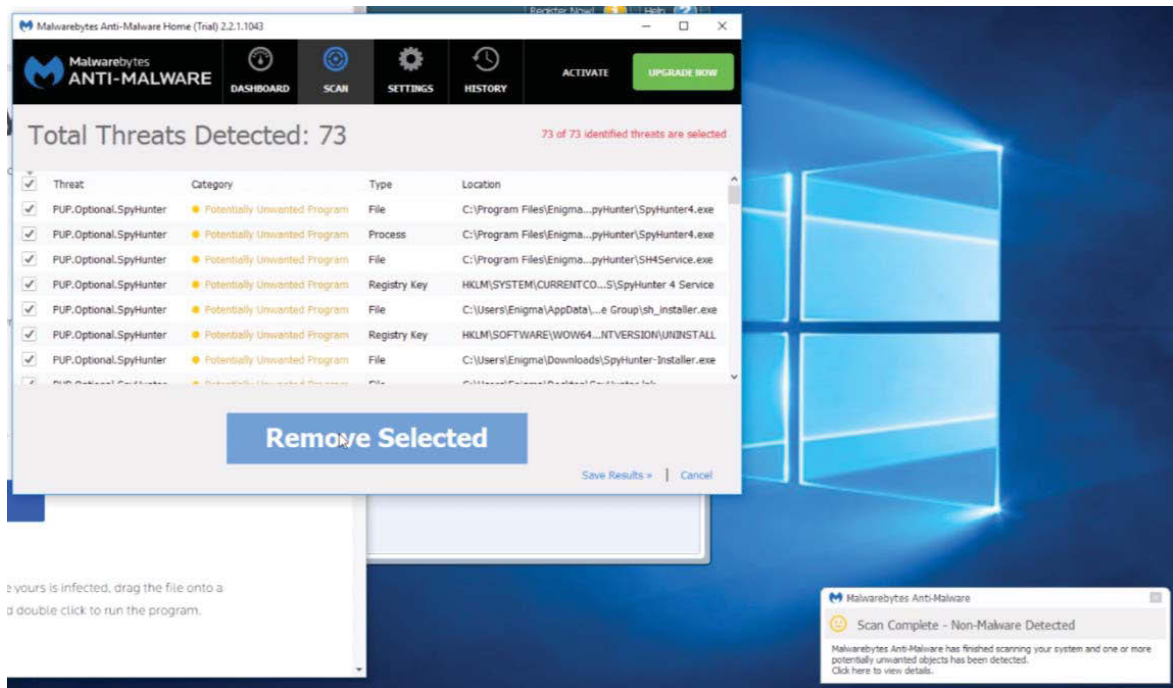
79. Numerous anti-malware products offered by companies other than ESG have been unaffected by Malwarebytes’ changed PUP criteria. Upon information and belief, MBAM does not detect as a PUP or flag as a “threat” any of the following anti-malware products which have similar characteristics to ESG’s SpyHunter product and therefore would be expected to have similar PUP detection results: Ad-Aware, AhnLab-V3, Avast, AVG, Avira, Bkav, Baidu, Bitdefender, CAT-QuickHeal, ClamAV, CMC_download, CMC_Install, Comodo, DrWeb, eScan, Emsisoft, ESET, F-Prot, F-Secure, Fortinet, G DATA, IKARUS, Jiangmin, K7AntiVirus, Kaspersky, Kingsoft, McAfee, NANO-Antivirus, nProtect, Panda, Qihoo-360, Rising, Sophos, SUPERAntiSpyware, Symantec, Tencent, TrendMicro, Trend Micro HouseCall, Vipre, VirBot, Windows Defender, and Zillya.

Malwarebytes Begins Detecting and Blocking SpyHunter and RegHunter

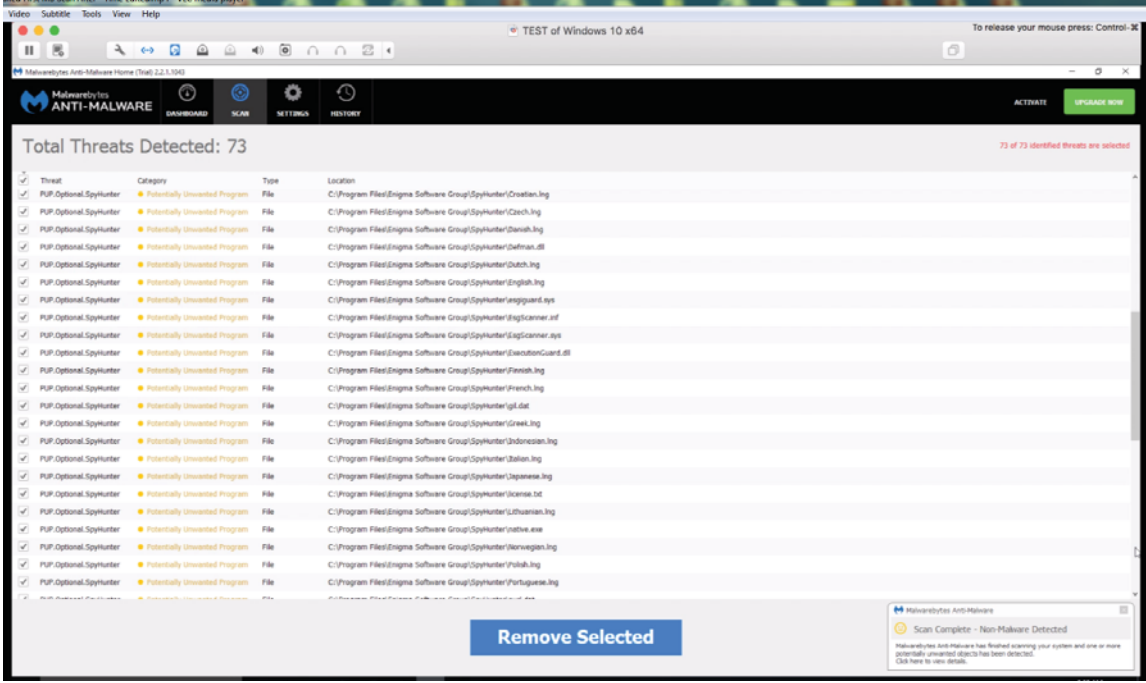
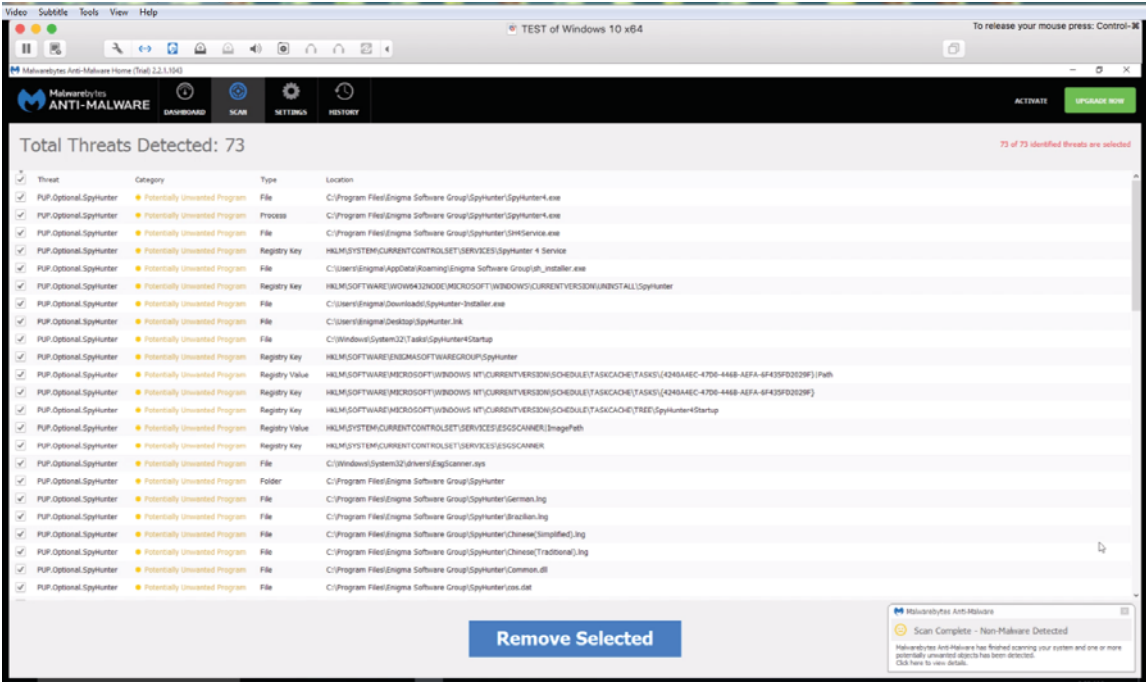
80. Once Malwarebytes announced its new PUP criteria on October 5, 2016, its programs began identifying and blocking SpyHunter and RegHunter.

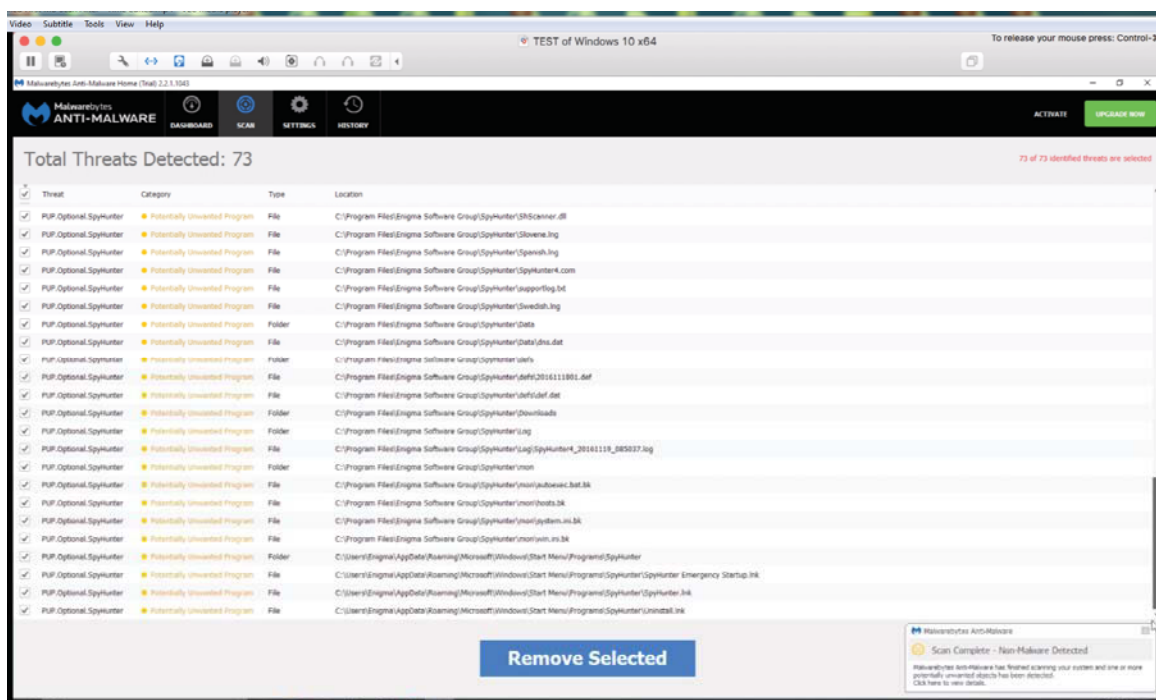
81. Immediately following Malwarebytes’ October 5, 2016 announcement, MBAM began detecting SpyHunter and RegHunter as PUPs, quarantining users’ existing SpyHunter and RegHunter programs, and blocking the installation of SpyHunter and RegHunter by new ESG customers.

82. For example, as depicted in the below screenshot, if a consumer already has downloaded, installed and paid for SpyHunter and runs an MBAM scan, MBAM displays a “Total Threats Detected” window, informing that user that SpyHunter is posing numerous “threats” to his or her computer:



83. If the user expands the “Total Threats Detected” window, as depicted in the below screenshots, the user can scroll through the “threats” and see that MBAM has identified numerous SpyHunter and ESG files, processes, registry keys, and registry values as PUPs:



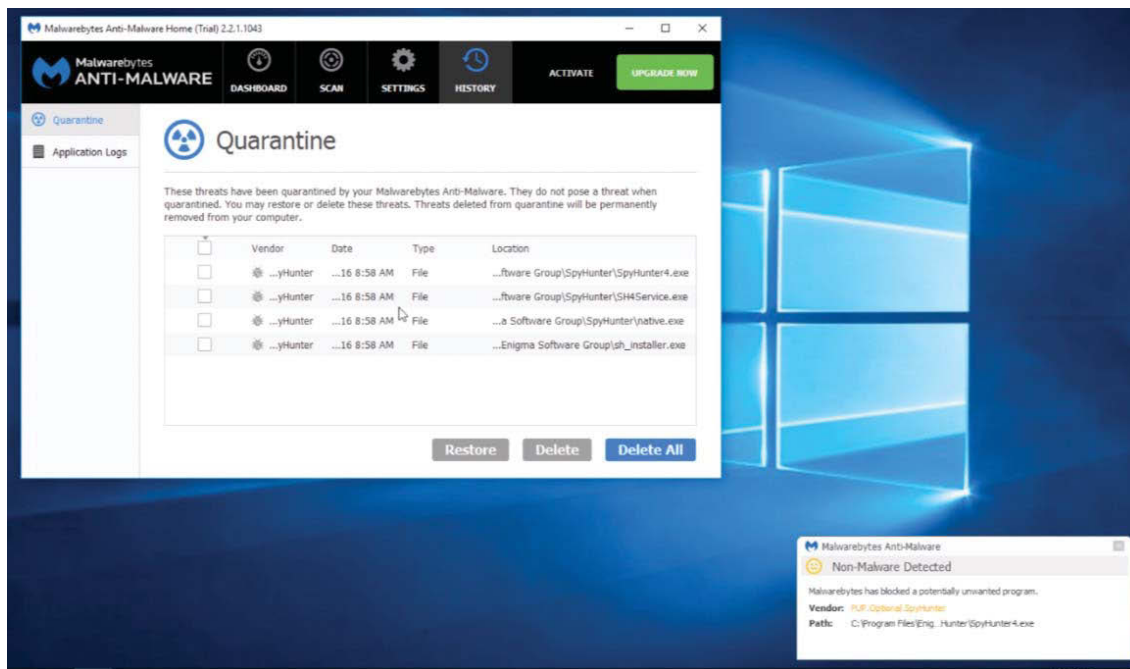


Notably, if the user’s machine is also infected with actual malware, the SpyHunter programs and files detected as “threats” would be buried amongst hundreds or even thousands of other identified “threats.” See ¶ 5 *supra*.

84. A big blue “Remove Selected” radio button at the bottom of the “Total Threats Detected” window prompts the user to remove the SpyHunter files and other items, which the MBAM program has automatically preselected for removal. Besides clicking “Remove Selected,” the user’s only option with respect to the detected “threats” is to ignore them by closing out of the “Total Threats Detected” window.

85. However, even if the user closes out of the “Total Threats Detected” window without electing to remove the “threats,” the next time he or she attempts to launch his or her SpyHunter application, he or she will receive an error message titled “Problem with Shortcut” that states: “The items ‘SpyHunter4.exe’ that this shortcut refers to has been changed or moved, so this shortcut will no longer work properly.”

86. Only if the user then opens MBAM's "Quarantine" window—which the user may not even know to do considering that the error message does not instruct the user to do so—will the user see that MBAM has quarantined his or her SpyHunter program, as depicted in the below screenshot:



87. MBAM explains to the user that the detected "threats," *i.e.* legitimate and non-malicious SpyHunter files, placed in the quarantine "do not pose a threat when quarantined" and if "deleted from quarantine will be permanently removed from [the user's] computer."

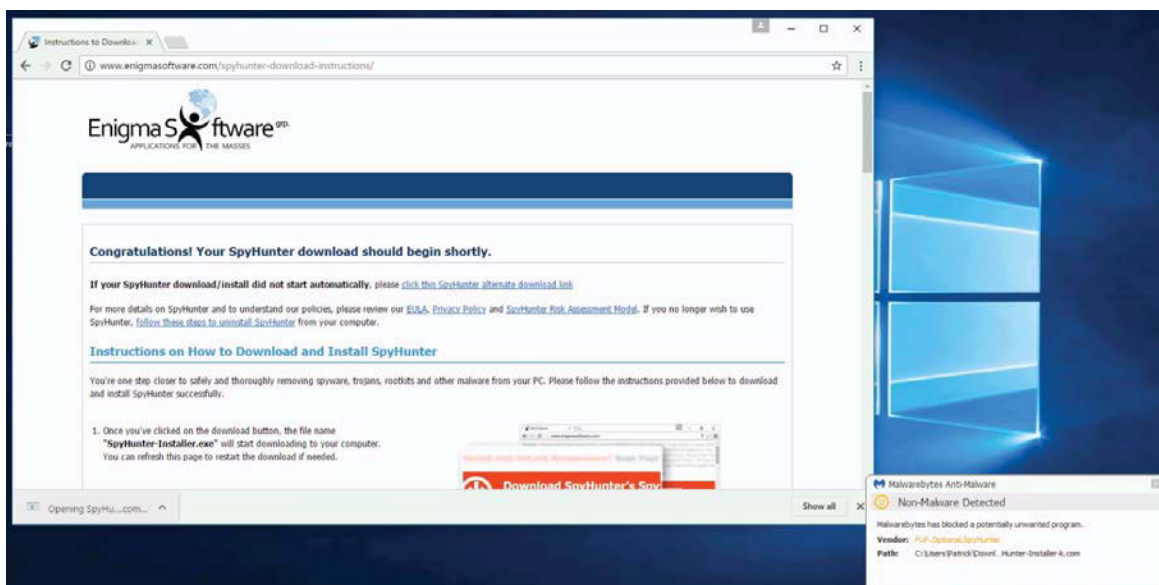
88. From the "Quarantine" window, the user can choose to "Restore" the quarantined SpyHunter files. However, even after clicking "Restore," a subsequent attempt by the user to re-launch the SpyHunter program will result in SpyHunter again being automatically quarantined by MBAM and the user again receiving the same "Problem with Shortcut" error message.

89. Even if the user restarts his or her computer, he or she will still be unable to launch SpyHunter upon reboot because numerous important SpyHunter files that are needed to launch the program have been removed.

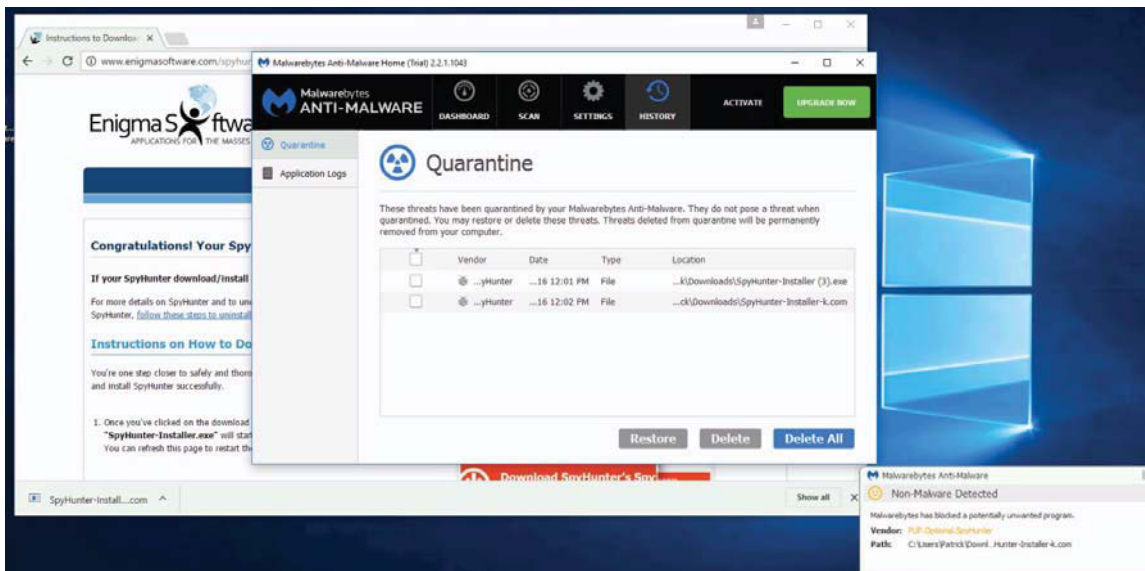
90. The only way for the user to re-enable SpyHunter is for the user to add the SpyHunter folder as a “Malware Exclusion” in the MBAM application. This is counterintuitive because PUPs are not malware. Regardless, the user may not know that he or she must, or even can, exclude certain items from detection by MBAM. Indeed, even upon consumer inquiry about why MBAM is blocking ESG’s programs—and upon expression by the consumer of his or her desire to use programs from both Malwarebytes and ESG—Malwarebytes does not provide exclusion instructions, or provides them in a way that is confusing and unhelpful to the user.

91. Moreover, even after the SpyHunter folder is added as a “Malware Exclusion,” subsequent MBAM scans continue to detect certain SpyHunter files and other items as PUPs, identifying them as “threats” for the user in the “Total Threats Detected” window.

92. Malwarebytes similarly is interfering with and disrupting a consumer’s ability to choose to download and install SpyHunter or RegHunter if that consumer already has MBAM installed on his or her computer. The below screenshot depicts MBAM blocking the SpyHunter installer file and displaying a pop-up that describes SpyHunter as a PUP:



93. If the user then clicks on the pop-up PUP warning—which a user may not know to do considering that MBAM does not instruct the user that clicking on the warning will lead to further information, or is even an option—MBAM displays its “Quarantine” window. As depicted in the below screenshot, the “Quarantine” window indicates that the SpyHunter installer file has been quarantined:



94. From the “Quarantine” window, the user can choose to “Restore” the quarantined SpyHunter files. However, even after clicking “Restore,” if the user downloads SpyHunter again, the pop-up PUP warning/quarantine process begins all over again, placing the user in a frustrating and unproductive cycle of restoring and re-downloading the file only to have the installer file blocked and quarantined each time.

95. Even adding the domain of the website from which the user is attempting to download SpyHunter to MBAM’s “Web Exclusions”—which, again, an MBAM user may not even know to do—does not stop MBAM from blocking the download and installation of the SpyHunter program.

96. MBAM's detection and blocking of SpyHunter and RegHunter as PUPs has been the subject of several threads on the Forums webpage of Malwarebytes' website. For example, on October 8, 2016, Malwarebytes forum "New Member" *pplcunha* posted to the thread Home > Malwarebytes Anti-Malware Support > Malwarebytes flags Spyhunter: "Since two days ago, Malwarebytes is flagging Spyhunter as a potentially undesired program. Any problems here?" Ex. 13. Malwarebytes "Elite Member" *pondus* responded that a PUP is a program that "comes bundled with some extra unwanted crap." *Id.* *pondus* continued: "Anyway, why use SpyHunter when you have Malwarebytes?" *Id.*

97. Contrary to *pondus*' suggestion, SpyHunter (and RegHunter and ESG's other programs) does not come bundled with unwanted software, utilities, toolbars, or other features.

98. Later on October 8, 2016, Malwarebytes "Special Ops" and "Trusted Advisor" *Aura* wrote in the thread: "Malwarebytes is now flagging SpyHunter products following a more aggressive stance against PUP. ... If you read the link provided by @pondus, SpyHunter fits in many of the criterias [sic] listed, so it's only normal for it to be classified as such." *Id.* *pplcunha* replied to *Aura*: "Thanks Aura for your reply and clarification. I still have a subscription with SpyHunter, but it will go off soon. I will be removing it soon." *Id.*

99. *Aura* concluded: "Make sure that your subscription gets cancelled for real when you do, since there's been a lot of report[s] in the past (and even today) of users still being charged by ESG for SpyHunter[.]" *Id.*

100. In addition to blocking SpyHunter and RegHunter through MBAM, Malwarebytes began detecting and blocking SpyHunter and RegHunter as PUPs through AdwCleaner just a week after Malwarebytes acquired that program.

ESG Receives Complaints and Refund Requests from New and Existing Customers

101. Beginning on October 7, 2016, ESG Technical Support began receiving complaints from customers about Malwarebytes' interference with their SpyHunter and RegHunter programs. Certain of the customers found it so difficult to exclude SpyHunter and RegHunter from MBAM's and/or AdwCleaner's PUP detection process that they requested immediate cancellation of their ESG accounts, nonrenewal of their program subscriptions, and refunds of their monthly subscription fees.

102. For example, on October 7, 2016, an ESG customer reported to ESG Technical Support that "Malwarebytes [was] removing SpyHunter." The ESG customer then provided ESG Technical Support a copy of an e-mail exchange with Malwarebytes Support agent Tom Mercado. The ESG customer had e-mailed Malwarebytes Support earlier that day under the subject "False Positive for SpyHunter v4":

I have been using your Premium product for a long time and have 149 days left.

Last night's Malwarebytes scan determined that another Product that also runs everynight [sic] - SpyHunter v4 Malware Security Suite from Enigma Software is a Potentially Unwanted Product. They have been running together without issue for many, many months.

On one machine I wasn't even able to deselect the threats, being told that items scheduled to be deleted upon reboot can't be deselected. And upon reboot all of my SpyHunter product is gone, even from Add & Remove products.

What would cause this sudden change in perception and what do your [sic] recommend[?]

Mercado responded: "Add it to our exclusions. We detect it as a PUP." He then provided links to articles on Malwarebytes' website purporting to provide, *inter alia*, "explanation on the

PUP.Optional detection category” and to instruct a user “how to add an IP\website or program to exclusion[.]”

103. The ESG customer replied to Malwarebytes Support:

Thank you for your response. However, it is clear (as of last night and not before) that Malwarebytes consider SpyHunter (a competing Malware protection program) a PUP. You say, “We detect it as a PUP”. Gee, I guess I already know that. But the fact is not until yesterday.

Could you please address the part of my question... What changed? I have been running these two programs side-by-side for over a year. NEVER a problem. Then last night- BANG. And in one case Malwarebytes proceeded to completely remove SpyHunter. Wouldn't even let me make SpyHunter an exclusion, as I explained. I am sure you are familiar with the error message - can't keep items that are scheduled to be removed upon reboot. UGH.

Either you folks changed your definitions or they changed their product during an update, and the indication is that it was Malwarebytes that made the change.

Please explain why sometime between October 5-7 things changed. Because something sure did.

Mercado replied by merely providing a link to another article on Malwarebytes' website and stating: “[T]hat software [SpyHunter] has always had dodgy, aggressive affiliate activities since as far back as I can recall and I've been at this for well over a decade.”

104. Also on October 7, 2016, an ESG customer who, upon information and belief, resides in the Bronx, New York contacted ESG Technical Support because “Malwarebytes [was] removing SpyHunter.”

105. On October 9, 2016, another ESG customer contacted ESG Technical Support to cancel her subscriptions to SpyHunter and RegHunter and obtain a refund due to Malwarebytes' detection and blocking of the ESG programs. Specifically, the ESG customer wrote:

Can you please cancel both of my prescriptions [sic] of spy hunter and reg hunter and refund my money as soon as possible that has recently been taken out of my account yesterday and a few days ago.

Both of them have just been removed by another antivirus software as it has picked up 380 viruses in both hunters after spy hunter updated and had to remove it/uninstall them both to completely get rid of these viruses. ...

I am very disappointed about all of this, because I did like your programs and they have worked well for me in the past.

106. Also on October 9, 2016, an ESG customer contacted ESG Technical Support to cancel his ESG account and refund his last payment. Specifically, he wrote:

Since Malware bytes and your spyware are not compatible. [sic] Please just cancel my account and if possible refund my last payment \$39.99 from safe cart. I really liked your programs and if and when you get the bugs worked out with malware Bytes please let me know as i [sic] will purchase again.

The customer then sent a follow-up message, stating: “Do NOT renew my account until you have the problems with Malware Bytes resolved[.] [I]t would be nice if you could refund my last payment since i was not able to run your software due to the Maleware Bytes problem.” *Id.*

107. On October 11, 2016, an ESG customer who, upon information and belief, resides in New York, New York contacted ESG Technical Support because “Malwarebytes [was] removing SpyHunter and RegHunter.”

108. On October 12, 2016, another ESG customer, who previously had to re-install his SpyHunter due to Malwarebytes identifying it as a PUP and uninstalling it, forwarded to ESG Technical Support an e-mail exchange between him and a Malwarebytes Support agent. He explained to ESG Technical Support that he had e-mailed Malwarebytes Support to “complain[] about their software calling SpyHunter a type of virus or PUP[.]” The Malwarebytes Support

agent had responded: “I can’t really comment on this. All I can say is that they meet our revised PUP criteria.” The ESG customer replied:

I understand what you are saying. But for the life of me I cannot understand why in the world would your software consider Spy Hunter as some sort of bad software or PUP. This is one of the most recognized detection software available and has worked wonderfully for me for more than 3 years.

109. On October 13, 2016, an ESG customer wrote to ESG Technical Support: “I cannot use spyware hunter, malware bytes treats it like malware[.] I would like to cancel my order please.”

110. On October 15, 2016, an ESG customer who, upon information and belief, resides in Brooklyn, New York wrote to ESG Technical Support: “Thanks for the support. However it seems that the malware bytes software is interfering with the spy hunter software. I am not too facile with removing programs on Windows 10. But I think the malware bytes suddenly became incompatible with spy hunter and screwed up the computer.”

111. On or about October 18, 2016, an ESG customer wrote to ESG Technical Support: “I wish to cancel my subscriptions to Spy Hunter ... and Reg Hunter ... because my software for Malware keeps uninstalling your softwares [sic] & I no longer have access. Please cancel SPY HUNTER & REG HUNTER asap.”

112. On October 21, 2016, an ESG customer who, upon information and belief, resides in Brooklyn, New York wrote to ESG Technical Support: “malwarebytes anti malware Premium-blocking spyhunter ‘PUP.OPTIONAL.SPYHUNTER.’”

113. On October 27, 2016, an ESG customer forwarded to ESG Technical Support an email exchange between him and Mercado, the same Malwarebytes Support agent that had previously communicated with at least one other ESG customer. In the exchange, the customer

wrote to Malwarebytes Support under the subject “Malwarebytes Malware Settings to Protect SpyHunter”:

I have been running SpyHunter, RegHunter and Malwarebytes Antimalware all together for sometime now and 2 days ago, SpyHunter and RegHunter were suddenly gone from my system.

I contact SpyHunter/RegHunter support and they got me going again and added that they were in dialogue with you - I hope the 2 of you can resolve this soon.

In the meantime is there anything you can provide me with a fix?

Mercado provided the same generic response he provided to the other ESG customer, directing the customer to add the programs to Malwarebytes’ “exclusions” and referring the customer to several articles on Malwarebytes’ website. *Id.*

114. When forwarding the e-mail exchange to ESG Technical Support, the customer made clear that Malwarebytes’ response was “not very helpful for a non-techie like [him],” stating: “It is not clear to me how to add Spyhunter and Reghunter to the Malwarebytes as PUP exclusion.”

115. On November 1, 2016, an ESG customer wrote to ESG Technical Support: “Just to check if there are undiscovered threats in my system, I runned [sic] AdwCleaner from Malwarebytes. This program reported SpyHunter and RegHunter as Potentially Unwanted Programs. I did not agree with that but Malwarebytes continues to assume that your software is Potentially Unwanted.” The customer then shared a copy of an e-mail from a Malwarebytes Support agent, who stated: “We do not recommend those programs or programs like that. We have flagged the program/s [sic] because they meet the standards set out on [www.malwarebytes.com/pup\[.\]](http://www.malwarebytes.com/pup[.])”

116. On November 4, 2016, another ESG customer wrote to ESG Technical Support: “I want a refund. I run Malwarebytes. You should state upfront that your software is not compatible.”

117. On November 5, 2016, an ESG customer who, upon information and belief, resides in New Hartford, New York, wrote to ESG Technical Support: “My problem is I download Spyhunter, but Malware keeps booting it out as a ‘potential threat’. I had them both downloaded for the year, now the problem happens after I try to reinstall Spyhunter. It installs but keeps getting booted off[.]”

118. Also on November 5, 2016, an ESG customer who, upon information and belief, resides in Haverstraw, New York, wrote to ESG Technical Support: “Please cancel my subscription to SPY Hunter. It was under automatic renewal, PLease [sic] takeautomatic [sic] renewal away from it. Reason is that I have Malware (Anti-malware) program installed on5 [sic] of my computers under one licenese [sic] and Spy Ware is not compatable [sic] with Malware. Please refund me by credit card charges.”

119. On November 7, 2016, an ESG customer wrote to ESG Technical Support:

I have tried to install the software of this renewal but it wasn’t posible [sic] because I have installed also in my PC another program, Malwarebytes, that is incompatible with yours.

As I don’t want to get rid of this software (Malwarebytes), that’s why I’ll have to cancell [sic] your suscription. [sic] If it’s not posible [sic] to cancel this renewal, please keep in my order history that this is my last renewal of your software and I don’t want to renewal [sic] it anymore.

120. On November 9, 2016, another ESG customer requested a refund on SpyHunter due to its incompatibility with Malwarebytes’ product. The customer wrote: “As soon as I send

this message, I'll uninstall Spyhunter. You can later contact me ... if the problem is resolved.

I'll look for the refund on my credit card."

121. On November 10, 2016, an ESG customer who, upon information and belief, resides in Schenectady, New York, wrote to ESG Technical Support:

my reghunter and spyhunter disapeeard [sic] from my computer.
... i ran a 'malwarebytes' scan and clicked yes to fix errors which
were all errors from reg and spy hunter, i didnt [sic] know what i
was doin [sic] so that probably why its gone or not functioning
right. what do i do ? [sic]

122. Also on November 10, 2016, an ESG customer who, upon information and belief, resides in Brooklyn, New York wrote to ESG Technical Support:

I used licensed Spy Hunter for a while but suddenly this software
was removed somehow - when clicking on icon error message
displayed - The item Spy Hunter4.exe that this shortcut refer to has
been changed or moved. I downloaded exe again and run it but got
error message: Malwarebytes blocked it as PUP program. Please
advise.

123. To date, ESG has been contacted about Malwarebytes' interference with SpyHunter and/or RegHunter by more than 300 customers, at least twenty (20) of which, upon information and belief, reside in New York. Some of those customers have requested refunds and cancellation or nonrenewal of their subscriptions and ESG is informed and believe that untold numbers of other potential customers have simply not purchased licenses to SpyHunter or RegHunter because of Malwarebytes' unlawful conduct described herein.

Malwarebytes has Harmed, and Continues to Harm, ESG

124. SpyHunter, RegHunter, and ESG's other products are legitimate. They pose no security threat to a user's computer and are not harassing in any way.

125. Malwarebytes knows ESG's products do not pose any security threat and are not harassing.

126. Malwarebytes has no objective, good faith basis to claim that ESG's products are "potentially unwanted programs." Indeed, as the consumer complaints identified above illustrate, consumers who have already downloaded (and paid for), or are trying to download, SpyHunter or RegHunter *want* those programs on their computer, a fact Malwarebytes knows.

127. There is no good faith basis to believe that ESG's products are "potentially unwanted programs." Malwarebytes has listed ESG's products as PUPs solely to bolster Bleeping's defense in the Bleeping Lawsuit and as an anticompetitive attempt to drive ESG out of business, to Malwarebytes' ultimate benefit.

128. Malwarebytes' unlawful conduct is willful and malicious.

129. Malwarebytes' unlawful conduct is causing and will continue to cause harm to ESG.

130. ESG has taken reasonable countermeasures to try to reduce the harm it has suffered, and continues to suffer, as a result of Malwarebytes' unlawful conduct, but the harm remains significant and continuing.

131. Shortly after Malwarebytes began unlawfully identifying SpyHunter and RegHunter as PUPs, ESG began suffering a drop in its sales of SpyHunter and RegHunter licenses.

132. Additionally, by recommending to users who have already purchased a SpyHunter or RegHunter license and installed the programs that they delete SpyHunter and RegHunter because they are a "threat," Malwarebytes has caused and will continue to cause ESG customers to request refunds for their previously-purchased licenses.

133. ESG has no adequate remedy at law for certain of the relief requested below.

FIRST CAUSE OF ACTION

(Violations of Lanham Act § 43(a))

134. ESG repeats and incorporates by reference all of the foregoing paragraphs as if fully set forth herein.

135. Malwarebytes' use in commerce of false and misleading statements about ESG, SpyHunter and RegHunter constitutes false advertising in violation of 15 U.S.C. § 1125(a)(1)(B).

136. Malwarebytes' use in commerce of false and misleading statements about ESG, SpyHunter and RegHunter is likely to deceive consumers as to the nature, quality and efficacy of SpyHunter and RegHunter, including causing consumers to believe that SpyHunter and RegHunter are malicious or a threat.

137. Such deception is material as it is likely to influence consumers not to purchase SpyHunter or RegHunter and/or do business with ESG and, instead, to continue to utilize and subscribe to Malwarebytes' products.

138. Malwarebytes' false and misleading statements have actually deceived or have the capacity to deceive a substantial portion of their intended audience, *i.e.*, users of MBAM and/or AdwCleaner who are also existing and/or prospective customers of ESG and users of SpyHunter and/or RegHunter.

139. Where a consumer already has SpyHunter and/or RegHunter on his or her computer, Malwarebytes' false and misleading statements are shown to the user ***every time*** he or she runs a MBAM or AdwCleaner scan.

140. Malwarebytes' false and misleading statements are shown to users of MBAM and/or AdwCleaner ***every time*** a user attempts to download and install SpyHunter or RegHunter.

141. Malwarebytes' false and misleading statements are shown to the consuming public, including persons not currently using MBAM and/or AdwCleaner, via various threads on

the Forums webpage of Malwarebytes' website and via the public announcement on Twitter by one of AdwCleaner's developers, now a Malwarebytes engineer and researcher.

142. Malwarebytes' false and misleading statements are part of an organized campaign by Malwarebytes to strengthen its position in the market for anti-malware and Internet security products by unfairly driving consumers away from ESG, SpyHunter and RegHunter and to Malwarebytes' products, including to its paid Premium MBAM program.

143. As a direct and proximate result of Malwarebytes' unlawful acts, ESG has suffered and will continue to suffer significant monetary and reputational injury, including losses of sales and a lessening of goodwill associated with its products, in amounts that will be proven at trial but that are believed to or will exceed \$75,000, exclusive of interest and costs.

SECOND CAUSE OF ACTION

(Violations of New York General Business Law § 349)

144. ESG repeats and incorporates by reference all of the foregoing paragraphs as if fully set forth herein.

145. Section 349 of New York's General Business Law prohibits the use of deceptive acts or practices in the conduct of business, trade or commerce, or in the furnishing of any service in the State of New York.

146. Malwarebytes' unfair competition through the wrongful detection of SpyHunter and RegHunter as PUPs via MBAM and AdwCleaner constitutes deceptive and unfair trade practices.

147. Each time a consumer who has MBAM and/or AdwCleaner installed and running on his or her computer attempts to download and install SpyHunter or RegHunter, MBAM and AdwCleaner display to the consumer the deceptive statement that SpyHunter and/or RegHunter is a PUP. In certain instances, MBAM and AdwCleaner even automatically block the download

and installation of SpyHunter and RegHunter without giving consumers a clear option to override the block.

148. Malwarebytes' statements that SpyHunter and RegHunter are PUPs and its blocking of program installations are materially misleading to consumers because these acts wrongly suggest that SpyHunter and RegHunter—two legitimate and highly regarded programs—are malicious or threats.

149. As a result, consumers are harmed by being misled on false pretenses into not downloading and using effective anti-malware software and by being prevented without their consent from installing the software.

150. ESG has been and continues to be injured as a result of Malwarebytes' deceptive and unfair trade practices, including through losses of sales and a lessening of goodwill associated with its products, in amounts that will be proven at trial but that are believed to or will exceed \$75,000, exclusive of interest and costs.

THIRD CAUSE OF ACTION

(Tortious Interference with Contractual Relations)

151. ESG repeats and incorporates by reference all of the foregoing paragraphs as if fully set forth herein.

152. ESG has contractually licensed the SpyHunter and RegHunter software to numerous customers.

153. Malwarebytes knows that prior to beginning its false detection and blocking of SpyHunter and RegHunter as PUPs and threats, certain users of MBAM contemporaneously used SpyHunter and/or RegHunter.

154. Malwarebytes knows that since it began falsely detecting and blocking SpyHunter and RegHunter as PUPS and threats, certain MBAM users desire to, and have attempted to, continue contemporaneous use of SpyHunter and/or RegHunter.

155. Malwarebytes knows that since it began falsely detecting and blocking SpyHunter and/or RegHunter as PUPs and threats, certain users of MBAM and/or AdwCleaner desire to, and have attempted to, download, install, and use SpyHunter and/or RegHunter.

156. Malwarebytes knows that users who have SpyHunter and/or RegHunter installed on their computers, or who are seeking to download and install SpyHunter and/or RegHunter, contractually license that software from ESG.

157. By displaying messages to MBAM and AdwCleaner users that either also have SpyHunter or RegHunter installed on their computer, or are seeking to install SpyHunter or RegHunter, that SpyHunter and RegHunter are PUPs and threats, and by automatically blocking the installation of SpyHunter and RegHunter without user consent, Malwarebytes has intentionally and maliciously (i) induced users to choose not to install SpyHunter and RegHunter or to delete SpyHunter and RegHunter and (ii) disabled SpyHunter and RegHunter programs that ESG customers have already paid to install and use, causing confusion and anger among ESG's customers.

158. By making false and misleading statements to the consuming public, including persons not currently using MBAM and/or AdwCleaner, via various threads on the Forums webpage of Malwarebytes' website and via the public announcement on Twitter by one of AdwCleaner's developers, now a Malwarebytes engineer and researcher, that SpyHunter and RegHunter are PUPs and threats, Malwarebytes has intentionally and maliciously induced

consumers to choose not to install SpyHunter and RegHunter or to delete SpyHunter and RegHunter.

159. ESG has already begun receiving customer complaints and requests for refunds, cancellation and nonrenewal as a result of Malwarebytes' unlawful conduct.

160. As a result of Malwarebytes' tortious interference, ESG has been damaged at least through loss of license fees in amounts that will be proven at trial but that are believed to or will exceed \$75,000, exclusive of interest and costs.

FOURTH CAUSE OF ACTION

(Tortious Interference with Business Relations)

161. ESG repeats and incorporates by reference all of the foregoing paragraphs as if fully set forth herein.

162. Certain consumers who use or seek to download and install SpyHunter or RegHunter are prospective customers of ESG who have not yet paid the SpyHunter or RegHunter license fees required to obtain full product functionality.

163. Malwarebytes knows that consumers using or seeking to download and install SpyHunter or RegHunter may enter into a paid business relationship with ESG.

164. By displaying messages to MBAM and AdwCleaner users that are using or seeking to download and install SpyHunter or RegHunter that SpyHunter and RegHunter are PUPs and threats, and by automatically blocking the installation of SpyHunter and RegHunter without user consent, Malwarebytes has intentionally interfered with the prospective business relationships between those users and ESG by inducing the users not to complete the installation and/or not to purchase licenses to SpyHunter and/or RegHunter.

165. By making false and misleading statements to the consuming public, including persons not currently using MBAM and/or AdwCleaner, via various threads on the Forums

webpage of Malwarebytes' website and via the public announcement on Twitter by one of AdwCleaner's developers, now a Malwarebytes engineer and researcher, that SpyHunter and RegHunter are PUPs and threats, Malwarebytes has intentionally and maliciously induced consumers to choose not to install SpyHunter and RegHunter or to delete SpyHunter and RegHunter.

166. Malwarebytes has acted solely out of malice in wrongfully and misleadingly informing consumers that SpyHunter and RegHunter are PUPs and threats, and automatically blocking their installation without user consent.

167. Malwarebytes' wrongfully and misleadingly informing users that SpyHunter and RegHunter are PUPs and threats, and automatically blocking their installation without user consent, is an improper and illegitimate means of competition that Malwarebytes undertook for the sole purpose of inflicting intentional harm upon ESG.

168. As a result of Malwarebytes' tortious interference, ESG has been damaged at least through loss of license fees in amounts that will be proven at trial but that are believed to or will exceed \$75,000, exclusive of interest and costs.

PRAYER FOR RELIEF

WHEREFORE, ESG respectfully requests that the Court enter judgment in its favor as follows:

- a. Declaring that Malwarebytes' conduct violates 15 U.S.C. § 1125(a);
- b. Declaring that Malwarebytes' conduct constitutes a violation of New York General Business Law § 349;
- c. Declaring that Malwarebytes' conduct constitutes tortious interference with contractual relations under the laws of the State of New York;

d. Declaring that Malwarebytes' conduct constitutes tortious interference with business relations under the laws of the State of New York;

e. Preliminarily and permanently enjoining Malwarebytes from programming MBAM and AdwCleaner to detect SpyHunter and RegHunter as PUPs and to notify users of that detection;

f. Preliminarily and permanently enjoining Malwarebytes from programming MBAM and AdwCleaner to prevent the installation of SpyHunter and RegHunter;

g. Awarding ESG damages in an amount proven at trial and believed to be in excess of \$75,000, plus interest;

h. Awarding ESG punitive damages;

i. Awarding ESG its attorneys' fees and costs incurred in bringing this action; and

j. Awarding such other and further relief as the Court deems proper.

JURY TRIAL DEMANDED

ESG demands a trial by jury of all issues so triable in this action.

Dated: New York, New York
December 7, 2016

Respectfully submitted,

By: /s/ Terry Budd

Terry Budd
Christopher M. Verdini
Anna Shabalov
Admitted Pro Hac Vice
K&L GATES LLP
210 Sixth Avenue
Pittsburgh, PA 15222
Telephone: 412.355.6500
Facsimile: 412.355.6501
terry.budd@klgates.com
christopher.verdini@klgates.com
anna.shabalov@klgates.com

&

Eric A. Prager
K&L GATES LLP
599 Lexington Avenue
New York, NY 10022
Telephone: 212.536.3900
Facsimile: 212.536.3901
eric.prager@klgates.com

&

Theodore J. Angelis
Admitted Pro Hac Vice
K&L GATES LLP
925 4th Avenue, Suite 2900
Seattle, WA 98104
Telephone: 206.370.8101
Facsimile: 206.370.6006
theo.angelis@klgates.com

Attorneys for Plaintiff